## REMARKS/ARGUMENTS

This Response is in reply to the Office Action dated June 30, 2005. This Response is submitted within the three month period for reply extending to September 30, 2005. Claims 1-16 remain pending.

### Rejections under 35 U.S.C. 102

Claims 1-16 were rejected under 35 U.S.C. 102(e) as being anticipated by Vanstone et al. ("Vanstone" hereafter) (U.S. Patent No. 6,446,207). These rejections are traversed.

Summary of Vanstone

Vanstone teaches a method for establishing a secure session between correspondents (12) and (14). Correspondent (12) maintains a long term private key (d) and a number of precomputed values ($dQ_B$) for use in facilitating signature validation with correspondent (14). Correspondent (14) maintains a public key ($Q_B$) and a databank that includes the long term private key (d) of correspondent (12). During establishment of the secure session, the correspondent (12) computes a session key (r) that is based on an instantly generated short term private key (k). Using the session key (r) and the short term private key (k), the correspondent (12) generates three signature components (e), (e'), and (s). Correspondent (12) then communicates its identification and the three signature components (e), (e'), and (s) to correspondent (14).

Upon receipt of the three signature components (e), (e'), and (s) and the identification of correspondent (12), correspondent (14) retrieves the long term private key (d) associated with correspondent (12). Using the received signature components (e') and (s), the retrieved long term private key (d), and the public key ($Q_B$), the correspondent

(14) computes a value (k'), which in the event of a successful authorization should match the short term private key (k) that was generated by correspondent (12). Using the computed value (k'), the correspondent (14) computes a value ($e'_{test}$) that should match the received signature component (e'). If the computed value ($e'_{test}$) and the received signature component (e') match, the secure session establishment continues. Otherwise, the secure session establishment fails.

In the event that ($e'_{test}$) and (e') match, the short term private key (k') as computed by correspondent (14) is verified. Therefore, (k')=(k). Then, using the verified short term private key (k'), the correspondent (14) computes the session key (r). Correspondent (14) then uses the session key (r) to send a secure authorization message to correspondent (12). Upon receipt of the secure authorization message, correspondent (12) uses the session key (r) to extract a challenge from the secure authorization message and return the extracted challenge to the correspondent (14). Upon receipt of the returned challenge at correspondent (14), a secure session is established between correspondents (12) and (14), wherein the session key (r) is used as an encryption key.

Arguments

With regard to claim 1, Vanstone does not teach signing an unsigned binary on a first computing device to obtain a first signature. Rather, Vanstone teaches generating a signature on a first computing device, i.e., correspondent (12), wherein the signature is based on an instantly generated short term private key. The signature generated by correspondent (12) in Vanstone is used for establishing a secure session between two corresponding computing systems, i.e., correspondents (12) and (14). The rather complex method disclosed by Vanstone for generating the signature components (e), (e'), and (s)

on correspondent (12), does not teach or suggest the signing of an unsigned binary to generate a signature as recited in claim 1.

Further with regard to claim 1, Vanstone does not teach downloading the first signature and the unsigned binary from the first computing device to a second computing device, wherein the first signature has been obtained by signing the unsigned binary on the first computing device. Vanstone's teachings in this regard are limited to transmitting the signature components (e), (e'), and (s) from the correspondent (12) to the correspondent (14). Vanstone does not include any disclosure that suggests the signature components (e), (e'), and (s) are obtained by signing an unsigned binary. Furthermore, Vanstone does not include any disclosure of such an unsigned binary being transmitted with the signature components (e), (e'), and (s) to the correspondent (14).

Further with regard to claim 1, Vanstone does not teach using a token coupled to the second computing device to sign the unsigned binary to obtain a second signature, wherein the unsigned binary has been downloaded to the second computing device from the first computing device. In the context of Vanstone, the correspondent (14) may represent a second computing device. Vanstone does not include any teaching of correspondent (14) operating to sign an unsigned binary that has been transmitted, e.g., downloaded, from correspondent (12). More particularly, Vanstone does not include any teaching of correspondent (14) operating to sign an unsigned binary to obtain a second signature. The operation of correspondent (14) to recreate the short term private key (k) generated by correspondent (12), as discussed above, simply does not teach use of a token to perform a signing operation, particularly wherein the signing operation is performed to sign the unsigned binary, as required by claim 1. Moreover, Vanstone does not even teach the unsigned binary as existing on correspondent (12) or as being downloaded from correspondent (12) to correspondent (14). Further with regard to claim 1, Vanstone does

not teach comparing the first and second signatures, wherein the first and second signatures have been generated in accordance with the other recited features of claim 1.

In accordance with the foregoing, Vanstone does not teach each and every feature of claim 1, as required to support a rejection under 35 U.S.C. 102. Therefore, the Applicants submit that claim 1 is patentable over Vanstone. Additionally, due to their dependence on claim 1, each of claims 2-8 includes all of the features recited in claim 1 and is patentable over Vanstone for at least the reasons provided for claim 1.

Claim 9 recites a computer readable medium having program code embodied therein that is configured to use a token to sign an unsigned binary. The computer readable code recited in claim 9 essentially causes the computer to perform the various operations as recited in claim 1. Therefore, the arguments present above with regard to claim 1 are equally applicable to corresponding operations caused by the computer readable code as recited in claim 9. Thus, the Applicants submit that claim 9 is patentable over Vanstone for at least the same reasons discussed above with respect to claim 1. Additionally, due to their dependence on claim 9, each of claims 10-16 includes all of the features recited in claim 9 and is patentable over Vanstone for at least the reasons provided for claim 9.

The Applicants submit that all of the pending claims are in condition for allowance. Therefore, a Notice of Allowance is requested. If the Examiner has any questions concerning the present Response, the Examiner is requested to contact the undersigned at (408) 774-6914. If any additional fees are due in connection with filing this Response, the Commissioner is also authorized to charge Deposit Account No. 50-0805 (Order No. SUNMP575). A duplicate copy of the transmittal is enclosed for this purpose.

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, LLP

Kenneth D. Wright
Reg. No. 53,795

710 Lakeway Drive, Suite 200
Sunnyvale, California 94086
Tel: (408) 749-6900
**Customer Number 32,291**